Singular values of some modular functions*

April 19, 2009

Noburo Ishii and Maho Kobayashi

1 Introduction

For a positive integer N, let $\Gamma_0(N)$ and $\Gamma_1(N)$ be the subgroups of $\mathrm{SL}_2(\mathbf{Z})$ defined by

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \;\middle|\; c \equiv 0 \mod N \right\},$$
$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \;\middle|\; a-1 \equiv c \equiv 0 \mod N \right\}.$$

We denote by $A_1(N)$ and $A_0(N)$ the modular function fields with respect to $\Gamma_1(N)$ and $\Gamma_0(N)$ respectively. Let $\mathfrak{E}$ be a set of triples of integers $\mathfrak{a} = [a_1, a_2, a_3]$ with the properties $0 < a_i \le N/2$ and $a_i \ne a_j$ for $i \ne j$. For an element τ of complex upper half plane $\mathfrak{H}$, we denote by L_τ the lattice in $\mathbf{C}$ generated by 1 and τ. Let $\wp(z; L_\tau)$ be the Weierstrass $\wp$-function relative to the lattice L_τ. For $\mathfrak{a} \in \mathfrak{E}$, consider a function $W_\mathfrak{a}(\tau)$ on $\mathfrak{H}$ defined by

$$W_\mathfrak{a}(\tau) = \frac{\wp(a_1/N; \tau) - \wp(a_3/N; \tau)}{\wp(a_2/N; \tau) - \wp(a_3/N; \tau)}.$$

This function is a modular function with respect to $\Gamma_1(N)$, referred in Chapter 18, §6 of Lang [6]. He pointed out that it is interesting to investigate its

*2000 *Mathematics Subject Classification* 11F03,11G15

special values at imaginary quadratic points. In [4] and [5], to construct generators of $A_1(N)$ and $A_0(N)$, we used the function $W_{\mathfrak{a}}(\tau)$ and the function $T_{\mathfrak{a}_1,\mathfrak{a}_2}(\tau)$ which is the trace of the product $W_{\mathfrak{a}_1}W_{\mathfrak{a}_2}$ ($\mathfrak{a}_i \in \mathfrak{C}$) relative to the extension $A_1(N)/A_0(N)$. Further we provided an explicit representation of the modular j-function $j(\tau)$ with those generators. In this article, we study the properties of singular values of $W_{\mathfrak{a}}$ and those of a function $T_{\mathfrak{A},F}$ which is a generalization of the function $T_{\mathfrak{a}_1,\mathfrak{a}_2}$. See §2 for the precise definition of $T_{\mathfrak{A},F}$. Our results in this article are as follows. In Theorem 3.7 and Corollary 4.6 we prove, for imaginary quadratic points $\alpha \in \mathfrak{H}$ and sets $\mathfrak{a}, \mathfrak{A}$ satisfying some conditions, that singular values $W_{\mathfrak{a}}(\alpha)$ are units of the ray class field $\mathfrak{K}_N$ modulo N over K and that singular values $T_{\mathfrak{A},F}(\alpha)$ are algebraic integers in $\mathfrak{K}_N$. In particular, consider the triples $\mathfrak{a}_1 = [2,3,1]$ and $\mathfrak{a}_2 = [2,5,1]$. Then we prove in Theorem 4.4 that $W_{\mathfrak{a}_1}(\alpha)$ and $W_{\mathfrak{a}_2}(\alpha)$ generate $\mathfrak{K}_N$ over the field $K(\exp(2\pi i/N))$. Let $A_0(N)_{\mathbf{Q}}$ be the subfield of $A_0(N)$ consisting of modular functions with Fourier coefficients in $\mathbf{Q}$. In Proposition 4.2 we show for prime numbers N that $A_0(N)_{\mathbf{Q}} = \mathbf{Q}(T_{\mathfrak{a}_1}, T_{\mathfrak{a}_2}) = \mathbf{Q}(T_{\mathfrak{a}_i}, T_{\mathfrak{a}_1,\mathfrak{a}_2})$ $(i = 1, 2)$. Further put $\mathfrak{A}_0 = [\mathfrak{a}_1, \mathfrak{a}_2]$ and $F_0 = X_1^m X_2^n$ for non-negative integers m and n. In Theorem 4.3, without the assumption N are prime, we show that $A_0(N)_{\mathbf{Q}} = \mathbf{Q}(j, T_{\mathfrak{A}_0,F_0})$. We deduce from those results that singular values of those functions generate ring class fields over K (see Theorem 4.7). Finally in §5 we study class polynomials of $T_{\mathfrak{A},F}$ with respect to Schertz N-systems.

In the followings, for a function $f(\tau)$ and a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$, we shall denote

$$f[A]_2 = f\left(\frac{a\tau+b}{c\tau+d}\right)(c\tau+d)^{-2} \text{ and } f\circ A = f\left(\frac{a\tau+b}{c\tau+d}\right).$$

2 Modular functions $W_{\mathfrak{a}}(\tau)$ and $T_{\mathfrak{A},F}(\tau)$

Let $W_{\mathfrak{a}}(\tau)$ be the function defined in §1. In [4], we showed the function $W_{\mathfrak{a}}$ is a modular function with respect to $\Gamma_1(N)$ and it has neither zeros nor poles on $\mathfrak{H}$. Let us consider the factor group $G(N) = \Gamma_0(N)/\{\pm E_2\}\Gamma_1(N)$, where E_2 is the unit matrix. Put $\mathfrak{S}_N = (\mathbf{Z}/N\mathbf{Z})^\times/\{\pm 1\}$. Then

$$G(N) \cong \left\{ \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{pmatrix} \middle| \lambda \in \mathfrak{S}_N \right\}.$$

For $\lambda \in \mathfrak{S}_N$, let $M_\lambda \in \Gamma_0(N)$ such that $M_\lambda \equiv \left(\begin{smallmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{smallmatrix}\right) \mod N$. For a tuple $\mathfrak{A} = [\mathfrak{a}_1, \ldots, \mathfrak{a}_n]$ ($\mathfrak{a}_i \in \mathfrak{E}$) and a polynomial $F = F(X_1, X_2, \ldots, X_n) \in \mathbf{Z}[X_1, X_2, \ldots, X_n]$, we define a function

$$T_{\mathfrak{A},F}(\tau) = \sum_{\lambda \in \mathfrak{S}_N} F(W_{\mathfrak{a}_1} \circ M_\lambda, \cdots, W_{\mathfrak{a}_n} \circ M_\lambda).$$

Then obviously $T_{\mathfrak{A},F}(\tau)$ is a modular function with respect to $\Gamma_0(N)$ and has no poles on $\mathfrak{H}$. For $\lambda \in \mathfrak{S}_N, \mathfrak{a} = [a_1, a_2, a_3] \in \mathfrak{E}$, define an element $\lambda\mathfrak{a}$ of $\mathfrak{E}$ by

$$\lambda\mathfrak{a} = [\{\lambda a_1\}, \{\lambda a_2\}, \{\lambda a_3\}],$$

where $\{\lambda a_i\}$ is the integer such that $\{\lambda a_i\} \equiv \pm\lambda a_i \mod N,\ 0 < \{\lambda a_i\} \leq \frac{N}{2}$.

Proposition 2.1. (i) *$W_{\mathfrak{a}}(M_\lambda \tau) = W_{\lambda\mathfrak{a}}(\tau)$.*

(ii) $$T_{\mathfrak{A},F}(\tau) = \sum_{\lambda \in \mathfrak{S}_N} F(W_{\lambda\mathfrak{a}_1}(\tau), \cdots, W_{\lambda\mathfrak{a}_n}(\tau)).$$

Proof. The assertion (i) is showed in §2 of [4]. The assertion (ii) is obvious from (i). □

We denote by $T_{\mathfrak{a}}$ and $T_{\mathfrak{a}_1,\mathfrak{a}_2}$ the function $T_{\mathfrak{A},F}$ with $\mathfrak{A} = [\mathfrak{a}], F = X_1$ and $\mathfrak{A} = [\mathfrak{a}_1, \mathfrak{a}_2], F = X_1X_2$ respectively.

3 Modular equations

Let j be the modular j-function. Let Γ be a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of finite index. For a modular function f with respect to Γ, we define the modular equation of f relative to j by

$$\Phi[f](X, j) = \prod_B (X - f \circ B),$$

where B runs over a transversal of the coset decomposition of $\mathrm{SL}_2(\mathbf{Z})$ by Γ. Obviously the coefficients of $\Phi[f](X, j)$ with respect to X are in $\mathbf{C}(j)$. If f has no poles on $\mathfrak{H}$, then the coefficients of $\Phi[f](X, j)$ are polynomials of j. Hereafter to avoid tedious notation, we denote by $\Phi_{\mathfrak{A},F}(X, j)$ the equation $\Phi[T_{\mathfrak{A},F}](X, j)$. Since $W_{\mathfrak{a}}$ and $T_{\mathfrak{A},F}$ have no poles on $\mathfrak{H}$, we have

$\Phi[W_{\mathfrak{a}}](X,j)$, $\Phi_{\mathfrak{A},F}(X,j) \in \mathbf{C}[j][X]$. We shall show that $\Phi[W_{\mathfrak{a}}](X,j)$ and $\Phi_{\mathfrak{A},F}(X,j) \in \mathbf{Z}[j][X]$ under some conditions imposed on N and $\mathfrak{A}$. For a positive divisor t of N, let Θ_t be a set of $\varphi((t,N/t))$ pairs of integers (u,v) such that $(u,t)=1$, $uv \equiv 1 \mod t$ and u are inequivalent to each other modulo $(t,N/t)$. For $(u,v) \in \Theta_t$ and $k \in \mathbf{Z}$, consider a matrix in $\mathrm{SL}_2(\mathbf{Z})$

$$B(t,u,v,k) = \begin{pmatrix} u & (uv-1)/t + uk \\ t & v+tk \end{pmatrix}.$$

We denote by $\mathfrak{M}_{\Theta_t}$ the set of matrices

$$\{B(t,u,v,k) \mid (u,v) \in \Theta_t,\ k \bmod N/(t^2,N)\}.$$

Lemma 3.1. (i) *The set of matrices* $\underset{t|N}{\cup}\mathfrak{M}_{\Theta_t}$ *is a transversal of the coset decomposition of* $\mathrm{SL}_2(\mathbf{Z})$ *by* $\Gamma_0(N)$.

(ii) *The set of matrices* $\{M_\lambda B \mid \lambda \in \mathfrak{S}_N, B \in \underset{t|N}{\cup}\mathfrak{M}_{\Theta_t}\}$ *is a transversal of the coset decomposition of* $\mathrm{SL}_2(\mathbf{Z})$ *by* $\Gamma_1(N)\{\pm E_2\}$.

Proof. The number of elements of the set is $\displaystyle\sum_{t|N} \frac{N}{(t^2,N)}\varphi((t,N/t))$. This is equal to $[\mathrm{SL}_2(\mathbf{Z}) : \Gamma_0(N)]$ (see Exercises 11.9 [1]). It is easy to see that any distinct matrices in the set $\underset{t|N}{\cup}\mathfrak{M}_{\Theta_t}$ are not in the same coset. Thus we have (i). The assertion (ii) is obvious from (i). $\square$

Let ℓ_t be an integer prime to t and ℓ_t^* an integer such that $\ell_t\ell_t^* \equiv 1 \mod t$. For the set Θ_t, put

$$\ell_t\Theta_t = \{(\ell_t^* u, \ell_t v) | (u,v) \in \Theta_t\}.$$

Then obviously the set of matrices $\underset{t|N}{\cup}\mathfrak{M}_{\ell_t\Theta_t}$ is also a transversal of the coset decomposition. For an integer s not congruent to $0 \mod N$, let

$$\phi_s(\tau) = \frac{1}{(2\pi i)^2}\wp\left(\frac{s}{N}; L_\tau\right) - 1/12.$$

Put $q = \exp(2\pi i\tau/N)$ and $\zeta = \exp(2\pi i/N)$. To consider the q-expansion of the function $\phi_s[B(t,u,v,k)]_2$, for an integer s, we define two integers $\{s\}$ and

$\mu(s)$ by the following conditions:

$$
\begin{aligned}
&0 \leq \{s\} \leq \frac{N}{2}, \quad \mu(s) = \pm 1, \\
&\begin{cases} \mu(s) = 1 & \text{if } s \equiv 0, N/2 \mod N, \\ s \equiv \mu(s)\{s\} \mod N & \text{otherwise.} \end{cases}
\end{aligned}
$$

By Lemma 1 of [4], we have, with $s^* = \mu(st)s(v + tk)$,

$$
\phi_s[B(t,u,v,k)]_2 = \tag{1}
$$

$$
\begin{cases} \dfrac{\zeta^{s^*}}{(1-\zeta^{s^*})^2} - \displaystyle\sum_{m=1}^{\infty}\sum_{n=1}^{\infty} n(1-\zeta^{s^*n})(1-\zeta^{-s^*n})q^{mnN} & \text{if } \{st\} = 0, \\ \\ \displaystyle\sum_{n=1}^{\infty} n\zeta^{s^*n}q^{\{st\}n} \\ \quad - \displaystyle\sum_{m=1}^{\infty}\sum_{n=1}^{\infty} n(1-\zeta^{s^*n}q^{\{st\}n})(1-\zeta^{-s^*n}q^{-\{st\}n})q^{mnN} & \text{otherwise.} \end{cases}
$$

In particular we note the function $\phi_s[B(t,u,v,k)]_2 \in \mathbf{Q}(\zeta)[[q]]$.

For an integer ℓ prime to N, let σ_ℓ be the automorphism of $\mathbf{Q}(\zeta)$ over $\mathbf{Q}$ defined by $\zeta^{\sigma_\ell} = \zeta^\ell$. On a function $f = \sum_m a_m q^m$ with $a_m \in \mathbf{Q}(\zeta)$, σ_ℓ acts by $f^{\sigma_\ell} = \sum_m a_m^{\sigma_\ell} q^m$.

Lemma 3.2. *Let ℓ be an integer prime to N and ℓ^* an integer such that $\ell\ell^* \equiv 1 \mod N$. Then for $(u,v) \in \Theta_t$ and $k \in \mathbf{Z}$,*

$$
\phi_s[B(t,u,v,k)]_2^{\sigma_\ell} = \begin{cases} \phi_{ls}[B(t,u,v,k)]_2 & \textit{if } \{st\} = 0, \\ \phi_s[B(t,\ell^*u,\ell v,\ell k)]_2 & \textit{if } \{st\} \neq 0 \end{cases}
$$

Proof. The q-expansion of $\phi_s[B(t,u,v,k)]_2^{\sigma_\ell}$ is given by substituting s^* by ℓs^* in the equation (1). If $\{st\} = 0$, then we see $\ell s^* = (\ell s)^*$. If $\{st\} \neq 0$, then $\ell s^* = \mu(st)\ell s(v + tk) = \mu(st)s(\ell v + \ell tk)$. By comparing the q-expansion of $\phi_{ls}[B(t,u,v,k)]_2$ or $\phi_s[B(t,\ell^*u,\ell v,\ell k)]_2$ in each case, we have our assertion. $\square$

We consider two subsets $\mathfrak{E}_1$ and $\mathfrak{E}_2$ of $\mathfrak{E}$ given by

$$\mathfrak{E}_1 = \{\mathfrak{a} \in \mathfrak{E} \mid (a_1 a_2 a_3, N) = 1\},$$
$$\mathfrak{E}_2 = \{\mathfrak{a} \in \mathfrak{E}_1 \mid (a_i \pm a_3, N) = 1 \text{ for } i = 1, 2\}.$$

It is noted $\mathfrak{E}_1 \neq \emptyset$ for $N \geq 7$ (resp.10) if N is odd (resp.even) and $\mathfrak{E}_2 \neq \emptyset$ for N such that $(N, 6) = 1, N \geq 7$. Further if N is a prime number and $N \geq 7$, then $\mathfrak{E}_1 = \mathfrak{E}_2 = \mathfrak{E}$.

Example 3.3. *Let* $\mathfrak{a}_1 = [2, 3, 1], \mathfrak{a}_2 = [2, 5, 1], \mathfrak{a}_3 = [1, (N-3)/2, (N-1)/2]$. *If* N *is a positive integer such that* $(N, 6) = 1, N \geq 7$. *Then* $\mathfrak{a}_1, \mathfrak{a}_3 \in \mathfrak{E}_2$. *Further if* $(N, 30) = 1$, *then* $\mathfrak{a}_2 \in \mathfrak{E}_2$. *The functions* $T_{\mathfrak{a}_i}$ *and* $T_{\mathfrak{a}_1,\mathfrak{a}_2}$ *are not constant. See Proposition 4.2.*

Proposition 3.4. *Let* ℓ *be an integer prime to* N *and* ℓ^* *an integer such that* $\ell\ell^* \equiv 1 \mod N$. *Further let* $(u, v) \in \Theta_t$ *and* $k \in \mathbf{Z}$.

(i) *For* $\mathfrak{a} = [a_1, a_2, a_3] \in \mathfrak{E}_1$, *we have*

$$(W_{\mathfrak{a}} \circ B(t, u, v, k))^{\sigma_\ell} = \begin{cases} W_{\ell\mathfrak{a}} \circ B(t, u, v, k) & \textit{if } t = N, \\ W_{\mathfrak{a}} \circ B(t, \ell^* u, \ell v, \ell k) & \textit{if } t \neq N, \end{cases}$$

where $\ell\mathfrak{a} = [\{\ell a_1\}, \{\ell a_2\}, \{\ell a_3\}]$.

(ii) *For a tuple* $\mathfrak{A} = [\mathfrak{a}_1, \ldots, \mathfrak{a}_n]$ $(\mathfrak{a}_i \in \mathfrak{E}_1)$, *we have*

$$(T_{\mathfrak{A},F} \circ B(t, u, v, k))^{\sigma_\ell} = \begin{cases} T_{\mathfrak{A},F} \circ B(t, u, v, k) & \textit{if } t = N, \\ T_{\mathfrak{A},F} \circ B(t, \ell^* u, \ell v, \ell k) & \textit{if } t \neq N. \end{cases}$$

Proof. By definition of $W_{\mathfrak{a}}$ we have

$$W_{\mathfrak{a}}(\tau) = \frac{\phi_{a_1}(\tau) - \phi_{a_3}(\tau)}{\phi_{a_2}(\tau) - \phi_{a_3}(\tau)}.$$

Therefore, (i) follows from Lemma 3.2 and (ii) is obvious from (i) and Proposition 2.1. □

It is noted that for $t = 1, N$ to obtain the results in Proposition 3.4, we do not need the condition $\mathfrak{a}_i \in \mathfrak{E}_1$.

Proposition 3.5. *For $\mathfrak{A}$ with $\mathfrak{a}_i \in \mathfrak{E}$, $T_{\mathfrak{A},F}$ and $T_{\mathfrak{A},F} \circ B(1,1,1,-1)$ have Fourier coefficients in* $\mathbf{Q}$.

Proof. Since $B(N,u,v,k) \in \Gamma_0(N)$, by Proposition 3.4 (ii), $T_{\mathfrak{A},F}^{\sigma_\ell} = T_{\mathfrak{A},F}$. By the same proposition, we have $(T_{\mathfrak{A},F} \circ B(1,1,1,-1))^{\sigma_\ell} = T_{\mathfrak{A},F} \circ B(1,\ell^*,\ell,-\ell)$. Since $B(1,1,1,-1)B(1,\ell^*,\ell,-\ell)^{-1} \in \Gamma_0(N)$, we see $(T_{\mathfrak{A},F} \circ B(1,1,1,-1))^{\sigma_\ell} = T_{\mathfrak{A},F} \circ B(1,1,1,-1)$. □

Put

$$\Phi[W_{\mathfrak{a}}](X,j) = X^{\Psi_1(N)} + \sum_{i=1}^{\Psi_1(N)} C[\mathfrak{a}]_i X^{\Psi_1(N)-i},$$
$$\Phi_{\mathfrak{A},F}(X,j) = X^{\Psi_0(N)} + \sum_{i=1}^{\Psi_0(N)} C_{\mathfrak{A},i} X^{\Psi_0(N)-i},$$

where $\Psi_0(N) = [\mathrm{SL}_2(\mathbf{Z}) : \Gamma_0(N)] = N \prod_{p|N} \left(1 + \dfrac{1}{p}\right)$, $\Psi_1(N) = [\mathrm{SL}_2(\mathbf{Z}) : \Gamma_1(N)] = \dfrac{\varphi(N)\Psi_0(N)}{2}$ and p are prime divisors of N.

Theorem 3.6. (i) *If $\mathfrak{a} \in \mathfrak{E}_1$, then the modular equation $\Phi[W_{\mathfrak{a}}] \in \mathbf{Q}[j][X]$. Further if N is odd and $\mathfrak{a} \in \mathfrak{E}_2$, then $\Phi[W_{\mathfrak{a}}] \in \mathbf{Z}[j][X]$.*

(ii) *Let $\mathfrak{A} = [\mathfrak{a}_1, \dots, \mathfrak{a}_n]$. If $\mathfrak{a}_k \in \mathfrak{E}_1$ for all k, then the modular equation $\Phi_{\mathfrak{A},F} \in \mathbf{Q}[j][X]$. Further if N is odd and $\mathfrak{a}_k \in \mathfrak{E}_2$ for all k, then $\Phi_{\mathfrak{A},F} \in \mathbf{Z}[j][X]$.*

Proof. We know the coefficients $C[\mathfrak{a}]_i$, $C_{\mathfrak{A},i} \in \mathbf{Q}(\zeta)((q))$. To show (i), we have only to prove that they are invariant under the action of σ_ℓ for all ℓ prime to N. By (i) of Proposition 2.1, we see $W_{\mathfrak{a}} \circ (M_\lambda B) = W_{\lambda\mathfrak{a}} \circ B$. Thus by Proposition 3.4, we have

$$(W_{\mathfrak{a}} \circ (M_\lambda B(t,u,v,k)))^{\sigma_\ell} = \begin{cases} W_{\mathfrak{a}} \circ (M_{\bar{\ell}\lambda} B(t,u,v,k)) & \text{if } t = N, \\ W_{\mathfrak{a}} \circ (M_\lambda B(t,\ell^* u,\ell v,\ell k)) & \text{if } t \neq N, \end{cases}$$

where $\bar{\ell}$ is the element of $\mathfrak{S}_N$ induced by ℓ. Since $C[\mathfrak{a}]_i$ is an elementary symmetric polynomial of $W_{\mathfrak{a}} \circ (M_\lambda B(t,u,v,k))$, we know that $C[\mathfrak{a}]_i^{\sigma_\ell} = C[\mathfrak{a}]_i$. Therefore We have $C[\mathfrak{a}]_i \in \mathbb{Q}[j]$. Assume that N is odd. Let us consider the q-expansions of the function $\phi_a[B]_2 - \phi_b[B]_2$ for $a, b \in \mathbf{Z}$, $(ab(a \pm b), N) = 1$ and

$B \in \mathfrak{M}_{\Theta_t}$. First of all, let $t \neq N$. Then $\{at\} \neq \{bt\}$. Let $l = \min(\{at\}, \{bt\})$. Then by (1), for an integer s

$$\phi_a[B]_2(\tau) - \phi_b[B]_2 = \pm\zeta^s q^l + O(q^{l+1}) \in \mathbf{Z}[\zeta][[q]].$$

Thus, $W_{\mathfrak{a}} \circ B \in \mathbf{Z}[\zeta]((q))$. Next we shall consider the case $t = N$. We can take $M_{\Theta_N} = \left\{\left(\begin{smallmatrix} 1 & 0 \\ N & 1 \end{smallmatrix}\right)\right\}$. Put $B = \left(\begin{smallmatrix} 1 & 0 \\ N & 1 \end{smallmatrix}\right)$. By (1), we see

$$\begin{aligned}
&\phi_a[B]_2(\tau) - \phi_b[B]_2 \\
&\qquad = \frac{\zeta^a(1-\zeta^{b-a})(1-\zeta^{b+a})}{(1-\zeta^a)^2(1-\zeta^b)^2} \\
&\qquad\quad - \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} n\{(1-\zeta^{an})(1-\zeta^{-an}) - (1-\zeta^{bn})(1-\zeta^{-bn})\}q^{mnN}.
\end{aligned}$$

Let

$$\begin{aligned}
\theta_{a,b} &= \frac{\zeta^a(1-\zeta^{b-a})(1-\zeta^{b+a})}{(1-\zeta^a)^2(1-\zeta^b)^2}, \\
h(q) &= -\sum_{m=1}^{\infty}\sum_{n=1}^{\infty} n\{(1-\zeta^{an})(1-\zeta^{-an}) - (1-\zeta^{bn})(1-\zeta^{-bn})\}q^{mnN}.
\end{aligned}$$

Then

$$\phi_a[B]_2 - \phi_b[B]_2 = \theta_{a,b}\big(1 - \frac{1}{\theta_{a,b}}h(q)\big).$$

Since $\dfrac{1-\zeta^s}{1-\zeta^r} \in \mathbf{Z}[\zeta]^\times$ for integers r, s such that $(rs, N) = 1$, we see

$$\frac{1}{\theta_{a,b}} = \frac{(1-\zeta^a)(1-\zeta^b)}{\zeta^a(1-\zeta^{b-a})(1-\zeta^{b+a})}(1-\zeta^a)(1-\zeta^b) \in \mathbf{Z}[\zeta].$$

Therefore for some $h(q), f(q) \in \mathbf{Z}[\zeta][[q]]$

$$W_{\mathfrak{a}} \circ B = \frac{\theta_{a_1,a_3}(1-h(q))}{\theta_{a_2,a_3}(1-f(q))} = \frac{\theta_{a_1,3}}{\theta_{a_2,3}}(1 + f(q) + f(q)^2 + \cdots)(1-h(q)).$$

Since

$$\frac{\theta_{a_1,3}}{\theta_{a_2,3}} = \frac{\zeta^{a_1}}{\zeta^{a_2}}\left(\frac{1-\zeta^{a_2}}{1-\zeta^{a_1}}\right)^2 \frac{(1-\zeta^{a_3-a_1})(1-\zeta^{a_3+a_1})}{(1-\zeta^{a_3-a_2})(1-\zeta^{a_3+a_2})} \in \mathbf{Z}[\zeta]^\times,$$

$W_{\mathfrak{a}} \circ B \in \mathbf{Z}[\zeta][[q]]$. Therefore by (i) of Proposition 2.1, we have $W_{\mathfrak{a}} \circ (M_\lambda B) \in \mathbf{Z}[\zeta]((q))$ for all $\lambda \in \mathfrak{S}_n$ and $B \in \cup_{t|N} \Theta_t$. Thus $C[\mathfrak{a}]_i \in \mathbf{Z}[\zeta]((q))$. By applying the above argument, we have $C[\mathfrak{a}]_i \in \mathbf{Z}[j]$. This shows (i). Next we shall prove (ii). By (ii) of Proposition 3.4, we have

$$\{(T_{\mathfrak{A},F} \circ B)^{\sigma_\ell} \mid B \in \mathfrak{M}_{\Theta_t}\} = \{T_{\mathfrak{A},F} \circ B \mid B \in \mathfrak{M}_{\ell\Theta_t}\}.$$

Since $\bigcup_{t|N} \mathfrak{M}_{\ell\Theta_t}$ is a transversal of coset decomposition of $\mathrm{SL}_2(\mathbf{Z})$ by $\Gamma_0(N)$, we obtain $C_{\mathfrak{A},i}^{\sigma_\ell} = C_{\mathfrak{A},i}$. This shows $C_{\mathfrak{A},i} \in \mathbf{Q}[j]$. If N is odd and $\mathfrak{a} \in \mathfrak{E}_2,\ \lambda \in \mathfrak{S}_N$, then $\lambda\mathfrak{a} \in \mathfrak{E}_2$. Proposition 2.1 shows $T_{\mathfrak{A},F} \circ B \in \mathbf{Z}[\zeta]((q))$. Therefore $C_{\mathfrak{A},i} \in \mathbf{Z}[\zeta]((q))$. Since $C_{\mathfrak{A},i}^{\sigma_\ell} = C_{\mathfrak{A},i}$, this shows $C_{\mathfrak{A},i} \in \mathbf{Z}[j]$. □

Let K be an imaginary quadratic field and $\mathfrak{K}_N$ the ray class field modulo N over K.

Theorem 3.7. *Assume that N is odd. Let α be an element of $\mathfrak{H}$ such that $K = \mathbf{Q}(\alpha)$.*

(i) *If $\mathfrak{a} \in \mathfrak{E}_2$, then $W_{\mathfrak{a}}(\alpha)$ is a unit of $\mathfrak{K}_N$.*

(ii) *Let $\mathfrak{A} = [\mathfrak{a}_1, \ldots, \mathfrak{a}_n]$. If $\mathfrak{a}_k \in \mathfrak{E}_2$ for all k, then $T_{\mathfrak{A},F}(\alpha)$ is an algebraic integer of $\mathfrak{K}_N$.*

Proof. By Complex multiplication theory, $j(\alpha)$ is an algebraic integer. Theorem 3.6 shows that $\Phi[W_{\mathfrak{a}}](X, j(\alpha))$ and $\Phi_{\mathfrak{A},F}(X, j(\alpha))$ are monic polynomials with algebraic integer coefficients. Thus $W_{\mathfrak{a}}(\alpha), T_{\mathfrak{A},F}(\alpha)$ are algebraic integers. By Corollary to Theorem 2 in §10.1 of [6], they are in $\mathfrak{K}_N$. Let $\mathfrak{a}' = [a_2, a_1, a_3]$. Since $W_{\mathfrak{a}}^{-1} = W_{\mathfrak{a}'}$ and $\mathfrak{a}' \in \mathfrak{E}_2$, $W_{\mathfrak{a}}(\alpha)^{-1}$ is an algebraic integer. Hence it is a unit. □

4 Ray class field and ring class field

Let K be a subfield of $\mathbf{C}$ and Γ a subgroup of $\mathrm{SL}_2(\mathbf{Z})$ of finite index. We denote by $A(\Gamma)_K$ the field of all modular functions with respect to Γ having Fourier coefficients in K. Further put $A_0(N)_K = A(\Gamma_0(N))_K,\ A_1(N)_K = A(\Gamma_1(N))_K$. Let $\zeta = \exp(2\pi i/N)$.

Proposition 4.1. *Put $\mathfrak{a}_1 = [2, 3, 1], \mathfrak{a}_2 = [2, 5, 1]$. If $N \geq 11, N \neq 12$, then*

$$A_1(N)_{\mathbf{Q}(\zeta)} = \mathbf{Q}(\zeta)(j, W_{\mathfrak{a}_1}) = \mathbf{Q}(\zeta)(j, W_{\mathfrak{a}_2}) = \mathbf{Q}(\zeta)(W_{\mathfrak{a}_1}, W_{\mathfrak{a}_2}).$$

Proof. The assertion is deduced from the result $A_1(N)_{\mathbf{C}} = \mathbf{C}(j, W_{\mathfrak{a}_i}) = \mathbf{C}(W_{\mathfrak{a}_1}, W_{\mathfrak{a}_2})$ and $W_{\mathfrak{a}_i} \in A_1(N)_{\mathbf{Q}(\zeta)} (i = 1, 2)$ in Lemma 1 and Theorems 1 and 5 of [4]. □

Let m and n be non-negative integers. Put $F = X_1^m X_2^n$ and $\mathfrak{A} = [\mathfrak{a}_1, \mathfrak{a}_2]$ with $\mathfrak{a}_1 = [2, 3, 1], \mathfrak{a}_2 = [2, 5, 1]$. For a while we shall consider the function $T_{\mathfrak{A},F}$. By Theorem 3.2 of [5], for any $\mathfrak{b} = [b_1, b_2, b_3] \in \mathfrak{E}$, the order of the q-expansion of $W_{\mathfrak{b}}$ at the point u/t is equal to $\min(\{tb_1\}, \{tb_3\}) - \min(\{tb_2\}, \{tb_3\})$. In particular, the order of q-expansion of $W_{\mathfrak{b}} \circ B(t, u, v, k)$ depends only on t and it equals to that of $W_{\mathfrak{b}}$ at the point $1/t$. For any integers a, b and c, we see $\{\{ab\}c\} = \{a\{bc\}\}$. Thus the order of q-expansion of $W_{\lambda\mathfrak{a}_i} \circ B(t, u, v, k)$ is that of $W_{\mathfrak{a}_i}$ at the point $1/\{\lambda t\}$. Let $\omega_i(\ell)$ be the order of q-expansion of $W_{\mathfrak{a}_i}$ at the point $1/\ell$ for $\ell \in \mathbf{Z},\ 1 \le \ell \le N/2$. By §3 of [4], we know $\omega_i(\ell) < 0$ if and only if $\ell > \frac{2N}{5}$ (resp. $\frac{3N}{7}$) for $i = 1$ (resp. $i = 2$). We have $\omega_i(\ell) = (i + 1)N - (2i + 3)\ell$ for $2N/5 < \ell \le N/2$ and ,in this range, obviously $\omega_i(\ell)$ is a strictly decreasing function of ℓ. Furthermore $\omega_i(\ell) \equiv 0 \mod (\ell, N)$.

Proposition 4.2. *Assume that N is a prime number and $N > 7$. Put $\mathfrak{a}_1 = [2, 3, 1], \mathfrak{a}_2 = [2, 5, 1]$ and $\mathfrak{a}_3 = [1, (N - 3)/2, (N - 1)/2]$. Then for $i = 1, 3$ and $j = 1, 2, 3$*

$$A_0(N)_{\mathbf{Q}} = \mathbf{Q}(T_{\mathfrak{a}_i}, T_{\mathfrak{a}_2}) = \mathbf{Q}(T_{\mathfrak{a}_j}, T_{\mathfrak{a}_1,\mathfrak{a}_2}).$$

Proof. Put $T_i = T_{\mathfrak{a}_i}$ for $i = 1, 2, 3$ and $T_4 = T_{\mathfrak{a}_1,\mathfrak{a}_2}$. Since N is a prime number, the group $\Gamma_0(N)$ has two cusps represented by $i\infty$ and 1. By Theorem 3.2 of [5], for any $\mathfrak{b} = [b_1, b_2, b_3] \in \mathfrak{E}$, $W_{\mathfrak{b}}$ is regular at the point $i\infty$. Therefore the functions T_i $(i = 1, \ldots, 4)$ are regular at $i\infty$. Let us denote by d_i the order of the pole of T_i at the cusp 1. We know $\omega_i(\lambda)$ has the smallest value only for $\lambda = (N - 1)/2$. Thus, we have $d_1 = (N - 5)/2, d_2 = (N - 7)/2$ and $d_4 = N - 6$. Let us determine d_3. The function $W_{\mathfrak{a}_3}$ has a pole of order $(N - 5)/2$ at 1. Let $\lambda > 1$. The function $W_{\lambda\mathfrak{a}_3}$ has a pole at 1 if $\lambda < \{\lambda(N - 1)/2\} < \{\lambda(N - 3)/2\}$ or $\lambda < \{\lambda(N - 3)/2\} < \{\lambda(N - 1)/2\}$. In the former case, the order d_λ of pole of $W_{\mathfrak{a}_3}$ at $1/\lambda$ is $\{\lambda(N - 1)/2\} - \lambda$. Since $\{\lambda(N - 1)/2\} < \{\lambda(N - 3)/2\}$, we know $\{\lambda(N - 1)/2\} \le (N - 3)/2$. Thus $d_\lambda < (N - 5)/2$. In the latter case, $d_\lambda = \{\lambda(N - 3)/2\} - \lambda$. Since $\lambda > 1, \{\lambda(N - 3)/2\} \le (N - 3)/2$, we know $d_\lambda < (N - 5)/2$. Therefore we have $d_3 = (N - 5)/2$. Proposition 3.5 shows that $T_i \in A_0(N)_{\mathbf{Q}}$. Since the modular curve $X_0(N)$ of $\Gamma_0(N)$ is defined over $\mathbf{Q}$, by Proposition 2.6 (a) in

Chapter II of [9], $d_i = [A_0(N)_{\mathbf{Q}} : \mathbf{Q}(T_i)]$. Since $((N-5)/2, (N-7)/2) = 1$ and $((N-5)(N-7), (N-6)) = 1$, we have our assertion. $\square$

Theorem 4.3. *Let m and n be non-negative integers. Assume that N does not divide* $5m+7n$ (resp. $2(5m+7n)$) *and* $N > 9$ (resp. 36) *in the case N is odd* (resp. even). *Put $\mathfrak{A} = [\mathfrak{a}_1, \mathfrak{a}_2]$ and $F = X_1^m X_2^n$. Further assume that $N \not\equiv 0 \mod 4$ in the case $m+n$ is even. Then we have $A_0(N)_{\mathbf{Q}} = \mathbf{Q}(j, T_{\mathfrak{A},F})$.*

Proof. Put $T = T_{\mathfrak{A},F}$. By Theorem 3 of Chapter 6 of [6], the field $A(\Gamma(N))_{\mathbf{Q}(\zeta)}$ is a Galois extension over $\mathbf{Q}(j)$ with the Galois group $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})/\{\pm E_2\}$ and the field $A_0(N)_{\mathbf{Q}}$ is the fixed field of the subgroup $\left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\}/\{\pm E_2\}$. Since $T \in A_0(N)_{\mathbf{Q}}$, to prove the assertions, it is sufficient to show that if $T \circ A = T$ for $A \in \mathrm{SL}_2(\mathbf{Z})$, then $A \in \Gamma_0(N)$. Let us consider the transversal $\{B(t,u,v,k)\}$ of the coset decomposition of $\mathrm{SL}_2(\mathbf{Z})$ by $\Gamma_0(N)$. Let $\omega(\ell)$ be the order of q-expansion of $W_{\mathfrak{a}_1}^m W_{\mathfrak{a}_2}^n$ at the point $1/\ell$. Then obviously $\omega(\ell) = m\omega_1(\ell) + n\omega_2(\ell)$. Let t be a divisor of N. If λ runs over $\mathfrak{S}_N$, then $\{\lambda t\}$ runs over all integers u such that $0 \le u \le N/2,\ (u,N) = t$. Therefore $d \ge \min\{\omega(\ell) \mid 0 \le \ell \le N/2,\ (\ell, N) = u\}$. Furthermore if $\omega(\ell)$ has the smallest value for only one ℓ, then we have equality. Let u_t be the greatest integer such that $(u_t, N) = t$ and $u_t \le N/2$. Let $t \ne N$. Assume that $T \circ B(t,u,v,k) = T$. Put $L = B(1,1,1,-1) = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$. Then $T \circ (B(t,u,v,k)L) = T \circ L$. We know $B(t,u,v,k)L = \begin{pmatrix} * & * \\ t(k+1)+v & -t \end{pmatrix}$. Let $\delta = (t(k+1)+v, N)$. Then we can take an integer ξ so that $\xi((k+1)t+v) + \delta t \equiv 0 \mod N$ and $(\xi, \delta) = 1$. For an integer η such that $\xi\eta \equiv 1 \mod \delta$, put $A = \begin{pmatrix} \eta & (\xi\eta - 1)/\delta \\ \delta & \xi \end{pmatrix}$. Since $B(t,u,v,k)LA^{-1} \in \Gamma_0(N)$, we have $T \circ A = T \circ L$. Let d be the order of q-expansion of $T \circ A$ and d_1 the order of q-expansion of $T \circ L$. In particular, the assumption implies that $d = d_1 \equiv 0 \mod \delta$. In the case $\delta \ne 1$, we shall show that $d \ne d_1$. If N is even, then $u_{N/2} = N/2$. If $\delta \ne N/2$, then u_δ is as follows.

N mod4	N/δ mod4	u_1	u_δ
$1,3$	$1,3$	$(N-1)/2$	$(N-\delta)/2$
2	$0,2$	$(N-4)/2$	$(N-4\delta)/2$
2	$1,3$	$(N-4)/2$	$(N-\delta)/2$
0	$1,3$	$(N-2)/2$	$(N-\delta)/2$
0	2	$(N-2)/2$	$(N-4\delta)/2$
0	0	$(N-2)/2$	$(N-2\delta)/2$

If we put $u_1 = (N-\epsilon)/2$ with $\epsilon = 1$ (resp. $2, 4$) in the case N is odd (resp. even), we see easily $d_1 = \omega(u_1) = ((5m+7n)\epsilon - (m+n)N)/2$ and $d \geq \min(0, \omega(u_\delta))$. It is noted that our assumption implies $d_1 < 0$. If $\delta = N$, then $d \geq 0$. Thus $d \neq d_1$. If $\delta = N/2$, then $d \equiv 0 \mod N/2$. By assumption, $d_1 \not\equiv 0 \mod N/2$. This implies $d \neq d_1$. Let $\delta \neq 1, N/2, N$. Except the case $N \equiv 2 \mod 4$ and $\delta = 2$, we have $u_\delta < u_1$. Thus $d \neq d_1$. In the exceptional case, we have $u_\delta > u_1$. Since there exists only one λ such that $\{2\lambda\} = u_2$, we have $d < d_1$. Let us consider the case $\delta = 1$. Then $d = d_1$. By (1), for a matrix $M = \begin{pmatrix} * & * \\ 1 & k \end{pmatrix}$ of $\mathrm{SL}_2(\mathbf{Z})$ and $0 < s \leq N/2$, we have

$$\varphi_s \circ M = \zeta^{s^*} q^s + \zeta^{-s^*} q^{N-s} + 2\zeta^{2s^*} q^{2s} + 2\zeta^{-2s^*} q^{2(N-s)} - q^N + (\text{higher terms}),$$

where $s^* = \mu(s)sk = sk$. If we put $s = s_r = \{ru_1\}$ for $r = 1, 2, 3, 5$, then $s_r = (N - r\epsilon)/2, s_r^* = ru_1k$ for $r = 1, 3, 5$ and $s_2 = \epsilon, s_2^* = -2u_1k$. Since $(N-\epsilon)/2 > 2\epsilon$, we have

$$\begin{aligned}(\varphi_{s_2} - \varphi_{s_1}) \circ M &= \zeta^{-2u_1k} q^{\epsilon}(1 + 2\zeta^{-2u_1k} q^{\epsilon} + O(q^{\epsilon+1})),\\ (\varphi_{s_3} - \varphi_{s_1}) \circ M &= \zeta^{3u_1k} q^{(N-3\epsilon)/2}(1 - \zeta^{-2u_1k} q^{\epsilon} + O(q^{\epsilon+1})),\\ (\varphi_{s_5} - \varphi_{s_1}) \circ M &= \zeta^{5u_1k} q^{(N-5\epsilon)/2}(1 + O(q^{\epsilon+1})),\end{aligned} \tag{2}$$

where the notation $O(q^n)$ denotes a q-series of order greater than or equal to n. Because the assumption for N implies $d_1 + \epsilon < 0, \omega(u_1 - 1)$, we see by (2),

$$T \circ M = \zeta^{-(5m+7n)u_1k} q^{d_1}(1 + (3m+2n)\zeta^{-2u_1k} q^{\epsilon} + O(q^{\epsilon+1})).$$

If we compare the coefficients of $T \circ A$ $(k = \xi)$ with those of $T \circ L (k = 0)$, we see $\zeta^{-(5m+7n)u_1\xi} = \zeta^{-2u_1\xi} = 1$. If $(5m+7n)$ is odd, then, since $(u_1, N) = 1$, we have $\xi \equiv 0 \mod N$. Since $\xi(t(k+1) + v) + t \equiv 0 \mod N$, we have $t \equiv 0$

mod N. This gives a contradiction. Obviously if $(5m+7n, N) = 1$, we have also a contradiction. For the case $5m+7n$ is even, we have $\zeta^{-2u_1\xi} = 1$. This shows $2t \equiv 0 \mod N$. Therefore if N is odd, we have a contradiction. Let $N \equiv 2 \mod 4$ and $t = N/2$. It is noted $\Theta_{N/2} = \{B(N/2, 1, 1, k) \mid k = 0, 1\}$. Since $(N/2, 2) = 1$, we can take integers x and y such that $(N/2)x + 2y = 1$. Consider a matrix $A = \begin{pmatrix} x & -1 \\ 2y & t \end{pmatrix}$ of $\mathrm{SL}_2(\mathbf{Z})$. It is easy to see that $B(N/2, 1, 1, k)AB(1, 1, 1, k(N/2)^2 - 1)^{-1}$, $AB(2, 1, 1, -y)^{-1} \in \Gamma_0(N)$. Therefore we have $T \circ B(1, 1, 1, k(N/2)^2 - 1) = T \circ B(2, 1, 1, -y)$. However the above argument for $N \equiv 2 \mod 4$ and $\delta = 2$ shows the order of q-expansions of the functions $T \circ B(1, 1, 1, k(N/2)^2 - 1)$ and $T \circ B(2, 1, 1, -y)$ are distinct. □

Theorem 4.4. *Let $\alpha \in \mathfrak{H}$ such that $\mathbf{Z}[\alpha]$ is a maximal order of K. Further let $\mathfrak{a}_1 = [2, 3, 1]$ and $\mathfrak{a}_2 = [2, 5, 1]$. If $N = 11$ or $N \geq 13$, then*

$$\mathfrak{K}_N = K(\zeta, j(\alpha), W_{\mathfrak{a}_1}(\alpha)) = K(\zeta, j(\alpha), W_{\mathfrak{a}_2}(\alpha)) = K(\zeta, W_{\mathfrak{a}_1}(\alpha), W_{\mathfrak{a}_2}(\alpha)).$$

Proof. Our assertion follows from Theorems 1 and 2 of [3] and Proposition 4.1. □

For a positive integer m, let O_m be the order of conductor m of K and R_m the ring class field associated with the order O_m. Consider the group

$$\Gamma^0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbf{Z}) \middle| b \equiv 0 \mod N \right\}.$$

Proposition 4.5. *Let $\theta \in \mathfrak{H}$ such that $O_f = \mathbf{Z}[\theta]$ and $f_\theta(X) = X^2 + BX + C$ $(B, C \in \mathbf{Z})$ the minimal polynomial of θ.*

(i) *If $h \in A_0(N)_{\mathbf{Q}}$ and h is pole-free at θ, then $h(\theta) \in R_{fN}$.*

(ii) *If $h \in A(\Gamma^0(N))_{\mathbf{Q}}$, h is pole-free at θ and $N|C$,then $h(\theta) \in R_f$.*

Proof. Let us use the notation in §2 of [3]. For a prime number p, consider groups

$$U_p = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Z}_p) \middle| c \in N\mathbf{Z}_p \right\},$$
$$V_p = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Z}_p) \middle| b \in N\mathbf{Z}_p \right\}.$$

Put $U = \prod_p U_p,\ V = \prod_p V_p$. Then U (resp.V) is the subgroup of $\prod_p \mathrm{GL}_2(\mathbf{Z}_p)$ with fixed field $F_0 = A_0(N)_{\mathbf{Q}}$ (resp.$F^0 = A(\Gamma^0(N))_{\mathbf{Q}}$). Let $O = O_f$ be the order of K of conductor f. By Theorems 5.5 and 5.7 of [8], we have an exact sequence

$$1 \longrightarrow O^* \longrightarrow \prod_p O_p^* \longrightarrow \mathrm{Gal}(K^{ab}/K(j(\theta)) \longrightarrow 1.$$

Let $g_\theta = \prod_p (g_\theta)_p : \prod_p O_p^* \longrightarrow \prod_p \mathrm{GL}_2(\mathbf{Z}_p)$ be the map defined by (4) and (5) in [3]. Since by the definition, for $s, t \in \mathbf{Z}_p$,

$$(g_\theta)_p(s\theta + t) = \begin{pmatrix} t - Bs & -Cs \\ s & t \end{pmatrix},$$

we have $(g_\theta)_p^{-1}(U_p) = (\mathbf{Z}_p^* + N\mathbf{Z}_p\theta) \cap O_p^* = (O_{fn})_p^*$. Therefore we have $g_\theta^{-1}(U) = \prod_p (O_{Nf})_p^*$. If $N|C$, then $(g_\theta)_p^{-1}(V_p) = O_p^*$ and $g_\theta^{-1}(V) = \prod_p O_p^*$. By class field theory the groups $\prod_p O_p^*$ and $\prod_p (O_{fN})_p^*$ correspond to $\mathrm{Gal}(K^{ab}/R_f)$ and $\mathrm{Gal}(K^{ab}/R_{fN})$ respectively. By Theorem 2 of [3], we see $R_f = K(F^0(\theta))$ and $R_{fN} = K(F_0(\theta))$. Therefore we have our assertions. $\square$

Corollary 4.6. *Let the notation be the same as in Proposition 4.5. Let* $\mathfrak{A} = [\mathfrak{a}_1, \ldots, \mathfrak{a}_n]$ *with* $\mathfrak{a}_i \in \mathfrak{E}_1$ *for all* i. *Then we have the followings.*

(i) $T_{\mathfrak{A},F}(\theta) \in R_{fN}$.

(ii) *If* $N|C$, *then* $T_{\mathfrak{A},F}(-1/\theta) \in R_f$.

Proof. Since $\Gamma^0(N) = S^{-1}\Gamma_0(N)S$ with $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, $T_{\mathfrak{A},F} \circ S$ is a modular function with respect to $\Gamma^0(N)$. By the result for $t = N$ in (ii) of Proposition 3.4, we know $T_{\mathfrak{A},F} \in \mathbf{Q}((q))$. Since $B(1,1,1,-1)S^{-1} \in \Gamma_0(N)$, we have $T_{\mathfrak{A},F} \circ S = T_{\mathfrak{A},F} \circ B(1,1,1,-1)$. By Proposition 3.5, we know $T_{\mathfrak{A},F} \in A_0(N)_{\mathbf{Q}}$ and $T_{\mathfrak{A},F} \circ S \in A(\Gamma^0(N))_{\mathbf{Q}}$. Our assertions follow from Proposition 4.5. $\square$

Theorem 4.7. *Put* $\mathfrak{a}_1 = [2,3,1], \mathfrak{a}_2 = [2,5,1], \mathfrak{a}_3 = [1,(N-3)/2,(N-1)/2]$ *and* $\mathfrak{A} = [\mathfrak{a}_1, \mathfrak{a}_2]$. *Put* $F = X_1^m X_2^n$ *with non-negative integers* m *and* n. *Let* $\theta \in \mathfrak{H}$ *such that* $O_f = \mathbf{Z}[\theta]$ *and* $f_\theta(X) = X^2 + BX + C$ $(B, C \in \mathbf{Z})$ *the minimal polynomial of* θ. *Then we have followings.*

(i) *If N is a prime number and $N > 7$, then*

$$R_{fN} = K(T_{\mathfrak{a}_i}(\theta), T_{\mathfrak{a}_2}(\theta)) = K(T_{\mathfrak{a}_j}(\theta), T_{\mathfrak{a}_1,\mathfrak{a}_2}(\theta)),$$

for $i = 1, 3$ and $j = 1, 2, 3$. Further if $N|C$, then

$$R_f = K(T_{\mathfrak{a}_i}(-1/\theta), T_{\mathfrak{a}_2}(-1/\theta)) = K(T_{\mathfrak{a}_j}(-1/\theta), T_{\mathfrak{a}_1,\mathfrak{a}_2}(-1/\theta)),$$

for $i = 1, 3$ and $j = 1, 2, 3$.

(ii) *Assume that N does not divide $5m + 7n$* (resp. $4(5m + 7n)$) *and $N > 9$* (resp. 36) *in the case N is odd* (resp. even). *Further assume that N is not divided by 4 in the case $m + n$ is even. Then $R_{fN} = K(j(\theta), T_{\mathfrak{A},F}(\theta))$. Further if $N|C$, then $R_f = K(j(\theta), T_{\mathfrak{A},F}(-1/\theta))$*

Proof. In the proof of Propositions 4.5 we showed $R_{Nf} = K(F_0(\theta)), R_f = K(F^0(\theta))$. Therefore the assertions follow from Propositions 4.2 and Theorem 4.3. □

5 Class polynomials of $T_{\mathfrak{A},F}$

Let O be the order of conductor f of an imaginary quadratic field K. Let D be the discriminant and $C(O)$ the (proper) ideal class group of O. We denote by $h(D)$ the class number of O. Let $\alpha \in K \cap \mathfrak{H}$ and $AX^2 + BX + C = 0$ be the primitive minimal equation with integral coefficients of α over $\mathbf{Q}$. If $D = B^2 - 4AC$, then we say α is an element of discriminant D. We put $I_\alpha = [A, (-B + \sqrt{D})/2] = \mathbf{Z}A + \mathbf{Z}((-B + \sqrt{D})/2)$. Then I_α is an ideal of O. To compute the singular values of the functions $T_{\mathfrak{A},F}$, we use an N-system for O introduced by Schertz [7].

Definition 5.1. *Let $\mathfrak{N}$ be a set of $h(D)$ elements $\alpha_i \in K \cap \mathfrak{H}$ of discriminant D. Let $A_iX^2 + B_iX + C_i = 0$ be the primitive integral minimal equation of α_i and $I_{\alpha_i} = [A_i, (-B_i + \sqrt{D})/2]$. We say $\mathfrak{N}$ is an N-system for O if following conditions are satisfied:*

1. $(A_i, N) = 1,\ N|C_i, B_i \equiv B_j \bmod 2N$ *for every i, j,*

2. *the set of ideals $\{I_{\alpha_i}\}$ is a transversal of $C(O)$.*

Let $\mathfrak{N}$ be an N-system for O. Then by Complex multiplication theory, for each $\alpha_i \in \mathfrak{N}$, $j(\alpha_i)$ is an algebraic integer and generates the ring class field R_f associated with the order of conductor f and they are conjugate to each other over $\mathbf{Q}$ (see §11.D of [1]). For singular values $T_{\mathfrak{A},F}(-1/\alpha_i)$ we have

Theorem 5.2. *Let N be a positive integer such that $\mathfrak{E}_2$ is not empty. Put $\mathfrak{A} = [\mathfrak{a}_1, \ldots, \mathfrak{a}_n]$ with $\mathfrak{a}_i \in \mathfrak{E}_2$. Let $\mathfrak{N} = \{\alpha_i\}$ be an N-system for O. Then we have $T_{\mathfrak{A},F}(-1/\alpha_i) \in R_f$ and they are conjugate to each other over K.*

Proof. Since $\Gamma^0(N) = S^{-1}\Gamma_0(N)S$ with $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, $T_{\mathfrak{A},F} \circ S$ is a modular function with respect to $\Gamma^0(N)$. In the proof of Corollary 4.6, we showed $T_{\mathfrak{A},F} \circ S \in \mathbf{Q}((q))$. Therefore the assertion follows from Theorem 3.1 of [2] and Theorem 3.7. □

For a modular function $g(\tau)$ with respect to $\Gamma_0(N)$ and an N-system $\mathfrak{N} = \{\alpha_i\}$, we define the class polynomial $H_{\mathfrak{N}}[g](X)$ of $g(\tau)$ by

$$H_{\mathfrak{N}}[g](X) = \prod_{i=1}^{h(D)} \left(X - g(-1/\alpha_i)\right).$$

The next assertion follows from Theorem 5.2.

Theorem 5.3. *Let O_K be the maximal order of K. Then the class polynomial $H_{\mathfrak{N}}[T_{\mathfrak{A},F}](X) \in O_K[X]$.*

Let B be an integer such that $B^2 \equiv D \pmod{4N}$. Proposition 3 of [7] shows the existence of N-system containing the number $(-B+\sqrt{D})/2$. By Lemma 3.1 of [10], we know the class polynomials of a modular function g related to N-systems depend only on integers B, considered mod $2N$. We shall fix an N-system containing $(-B+\sqrt{D})/2$ and denote it by $\mathfrak{N}_B$. In the followings, we give some examples of modular equations and class polynomials of the functions $f = T_{\mathfrak{a}}$ or $T_{\mathfrak{a}_1,\mathfrak{a}_2}$. We shall denote by $H_B(X)$ the class polynomial $H_{\mathfrak{N}_B}[f]$ in the case the function f is clearly indicated and any confusion can not occur.

Example 5.4. (1) *Let $N = 7, \mathfrak{a} = [2,3,1]$. Consider the function $T_{\mathfrak{a}}$. Then the modular equation $\Phi(X,j)$ of $T_{\mathfrak{a}}$ is given by*

$$\Phi(X,j) = X^8 - 36X^7 + 546X^6 - 4592X^5 + 23835X^4 - 80304X^3 + 176050X^2 - (j+232500)X + 140625 + 8j.$$

(a) *Let* $D=-3, B=5$. *Then* $h(-3)=1, \mathfrak{N}_5=\{(-5+\sqrt{-3})/2\}$. *We have the class polynomial*

$$H_5(X)=X-3(1+\sqrt{-3})/2.$$

Thus $T_{\mathfrak{a}}((5+\sqrt{-3})/14)=3(1+\sqrt{-3})/2$. *Since* $j((1+\sqrt{-3})/2)=0$, *we have* $\Phi(X,0)=(X^2-3X+9)(X^2-11X+25)^3$. *In fact,* $T_{\mathfrak{a}}((5+\sqrt{-3})/14)$ *is a root of the factor* $X^2-3X+9=0$.

(b) *Let* $D=-59, B=5$. *Then we have* $h(-59)=3$ *and*

$$\mathfrak{N}_5=\{(-5+\sqrt{-59})/2,(-5+\sqrt{-59})/6,(23+\sqrt{-59})/6\}$$
$$H_5(X)=X^3+\frac{15-7\sqrt{-59}}{2}X^2+\frac{-357+45\sqrt{-59}}{2}X+\frac{717+\sqrt{-59}}{2}.$$

(2) *Let* $N=13, D=-3, B=7, \mathfrak{a}=[5,3,1]$. *Take* $\mathfrak{N}_7=\{(-7+\sqrt{-3})/2\}$. *Then the modular equation* $\Phi(X,j)$ *of* $T_{\mathfrak{a}}$ *and the value* $T_{\mathfrak{a}}(7+\sqrt{-3})/26)$ *are given by*

$$\Phi(X,j)=(X^2-9X+27)(X^4-21X^3+167X^2+-604X+848)^3-j(X-7),$$
$$T_{\mathfrak{a}}((7+\sqrt{-3})/26)=(9+3\sqrt{-3})/2.$$

Thus in fact $T_{\mathfrak{A},F}((7+\sqrt{-3})/26)$ *is a root of* $X^2-9X+27=0D$

(3) *Let* $N=11,\ \mathfrak{a}=[2,5,1], D=-7, B=9$. *Then* $\mathfrak{N}_9=\{(-9+\sqrt{-7})/2\}$ *and we have* $T_{\mathfrak{a}}((9+\sqrt{-7})/44)=(5+\sqrt{-7})/2$ *and the modular equation*

$$\begin{aligned}\Phi(X,j)&=X^{12}-84X^{11}+2970X^{10}-57772X^9+680559X^8-5062728X^7\\&-(22j-24250028)X^6+(561j-75844824)X^5-(2981j-157525071)X^4\\&-(1177j+217265444)X^3+(26477j+193124250)X^2\\&-(j^2+31316j+101227452)X+18j^2+4261j+24137569.\end{aligned}$$

Since $j((1+\sqrt{-7})/2)=-15^3$, *we have*

$$\begin{aligned}\Phi(X,-15^3)&=(X^{10}-79X^9+2567X^8-44305X^7+438498X^6-2515798X^5\\&+8237304X^4-16425295X^3+19561039X^2+15914486X+26848493)\\&\times(X^2-5X+8).\end{aligned}$$

Therefore, we know $T_{\mathfrak{a}}((9+\sqrt{-7})/44)$ *is a root of the factor* X^2-5X+8.

Example 5.5. *Let* $N=11,\ \mathfrak{a}=[2,3,1], \mathfrak{b}=[2,3,5]$. *Consider the function* $T_{\mathfrak{a},\mathfrak{b}}$. *Then we give the coefficients* C_i *of the modular equation* $\Phi(X,j)=X^{12}+$

$\sum_{i=1}^{12} C_i X^{12-i}$ *in the table below.*

(1) *Let* $D = -83, B = 7$. *Then we have* $h(-83) = 3$ *and*

$$\mathfrak{N}_7 = \{(-7+\sqrt{-83})/2, (-7+\sqrt{-83})/6, (-29+\sqrt{-83})/6\},$$
$$H_7(X) = X^3 - (361481 + 7136\sqrt{-83})X^2 + (57020581 + 25984608\sqrt{-83})X$$
$$+ 1683573861 - 404390656\sqrt{-83}.$$

(2) *Let* $D = -39, B = 7$. *Then we have* $h(-39) = 4$ *and*

$$\mathfrak{N}_7 = \{(-7+\sqrt{-39})/2, (-7+\sqrt{-39})/4, (-29+\sqrt{-39})/4, (-51+\sqrt{-39})/8\},$$
$$H_7(X) = X^4 + (-4720 + 231\sqrt{-39})X^3 + (1491643 - 329343\sqrt{-39})X^2/2$$
$$+ (-38934427 + 9970611\sqrt{-39})X/2 + 64994911 - 47480958\sqrt{-39}.$$

i	C_i	i	
1	3660	2	4754178
3	$21879j + 2517699932$	4	$8917579j + 450023862255$
5	$10912j^2 - 21727187108j + 28522470464664$		
6	$18536243j^2 + 439266301210j + 155307879800348$		
7	$1419j^3 + 6356028822j^2 - 4268224633178j - 22718073239498472$		
8	$1663761j^3 + 70427463557j^2 - 129554423289764j + 430444117263292143$		
9	$66j^4 - 100966360j^3 + 544875974962j^2 + 1322596244939332j - 4047340123195216100$		
10	$82687j^4 - 2985616392j^3 + 3765768493971j^2 - 9777105305922130j + 21981914597781276930$		
11	$j^5 + 1956838j^4 - 26707875453j^3 + 49826805469384j^2 + 21725643544520963j$ -67067772106836815988		
12	$1229j^5 + 29053078j^4 - 41072974661j^3 - 92728235099098j^2 + 68572479313531217j$ $+93554961663154376449$		

Example 5.6. *Let* $N = 17, \mathfrak{a} = [1, 2, 7], \mathfrak{b} = [1, 2, 3]$. *Consider the function* $T_{\mathfrak{a},\mathfrak{b}}$. *Let* $D = -84, B = 8$. *Then we have* $h(-84) = 4$ *and*

$$\mathfrak{N}_8 = \{-8+\sqrt{-21}, (43+\sqrt{-21})/11, (-8+\sqrt{-21})/5, (9+\sqrt{-21})/3\},$$
$$H_8(X) = X^4 + (779 - 157\sqrt{-21})X^3 + (-41194 - 175\sqrt{-21})X^2$$
$$+ (690208 + 81256\sqrt{-21})X - 3246464 - 566976\sqrt{-21}.$$

References

[1] D.Cox, Primes of the form $x^2 + ny^2$, A Wiley-Interscience Publication, John Wiley and Sons,Inc.,1989

[2] A.Enge and R.Schertz, Constructing elliptic curves over finite fields using double eta-quotients, J.Théor.Nombres Bordeaux 16 (2004), 555–568.

[3] A.Gee, Class invariants by Shimura's reciprocity law, J.Théor.Nombres Bordeaux 11 (1990),45-72.

[4] N.Ishida and N.Ishii, Generators and defining equation of the modular function field of the group $\Gamma_1(N)$, Acta Arith. 101.4 (2002),303-320.

[5] N.Ishii, Rational expression for J-invariant function in terms of generators of modular function fields, Int.Math. Forum 2 (2007) no. 38, 1877 - 1894.

[6] S.Lang, Elliptic Functions, Springer-verlag,1987.

[7] R.Schertz, Weber's class invariants revisited, J.Théor. Nombres de Bordeaux 14(1) (2002), 325–343.

[8] G.Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, Iwanami-Shoten and Princeton University Press,1971.

[9] J.Silverman, The Arithmetic of Elliptic curves, Springer-verlag,1986.

[10] S.Yoshimura,A.Comuta and N.Ishii, N-systems,class polynomials of double eta-quotients and singular values of j-invariant function, Int.Math.Forum 4 (2009) no.8,367-376.

Faculty of Liberal arts and Sciences
Osaka Prefecture University
1-1 Gakuen-cho, Naka-ku Sakai
Osaka, 599-8531 Japan
e-mail: ishii@las.osakafu-u.ac.jp

Graduate School of Science
Osaka Prefecture University
1-1 Gakuen-cho, Naka-ku Sakai
Osaka, 599-8531 Japan